CIRCUIT DESIGN METHOD, APPARATUS, AND PROGRAM

ABSTRACT OF THE DISCLOSURE

A circuit design method able to design a processing circuit for processing a finite field with fewer circuit design elements and in a smaller size than the past comprising obtaining a first primitive root α_1 on the basis of a first polynomial for a first extension from a first finite field to a second finite field, obtaining a second primitive root α_2 on the basis of a second polynomial for a second extension from the second finite field to a third finite field, wherein a coefficient of a 0-th term is defined using the first primitive root α_1 obtained above and the coefficient of the 0-th term of the first polynomial, defining processing on the third finite field using a base expressed using the second primitive root α_2, and designing the processing circuit for performing that processing.